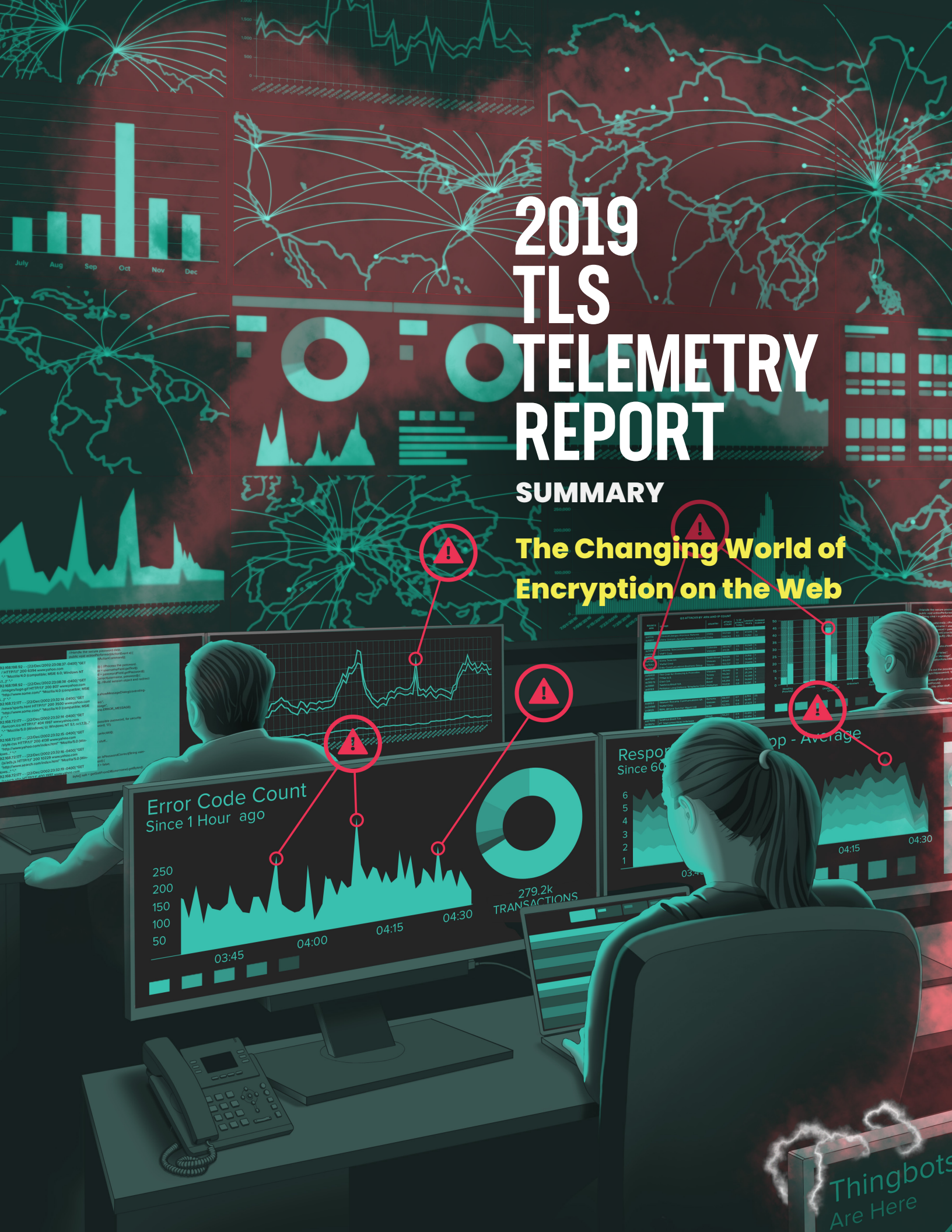


2019 TLS TELEMETRY REPORT

SUMMARY

The Changing World of Encryption on the Web

Authors

David Warburton is a Senior Threat Research Evangelist with F5 Labs with over 20 years' experience in IT and security. A regular speaker at industry events and contributor to online and broadcast media, he was responsible for the design of a public cloud platform and for helping large government organizations adapt and improve their security posture. He also recently completed an MSc in Information Security with Royal Holloway University where his thesis was on the use of cryptography in IoT.

Contributors

Remi Cohen | *Threat Research Evangelist, F5*

Debbie Walkowski | *Threat Research Evangelist, F5*

Business and Data Partners

GitHub

Founded in 2019, the **GitHub Security Lab** is a dedicated team of security researchers with the mission to help secure the open source ecosystem. To that end, the team hunts for high impact security vulnerabilities in open source software, builds tools that help secure code at scale, and actively partners with security teams across the industry to foster connections between the security research community and the software development community.

TABLE OF CONTENTS

YEARS OF PROGRESS

Let's Encrypt

Let's Encrypt allows creation of wildcard certificates for the first time since it began its automated certificate authority.

Certificate Transparency

Chrome, the world's most popular browser, now requires certificate transparency for any newly created certificate.

Google Highlights Insecure Sites

All non-encrypted sites are marked "insecure" in Chrome browsers starting July 24th.

Encrypted SNI Proposed

A new protocol is proposed to encrypt the server name indicator header (part of the TLS handshake).

WoSign and StartCom Untrusted

Due to repeated lapses of security related to their creation and management of certificates, major browsers distrust these two certificate authorities.

TLS 1.3

After 5 years of discussions and 10 years after the release of TLS 1.2, the new version of the web encryption protocol is ratified as RFC8446.

Variation on Lucky13 Attack

Researchers publish a paper that affects CBC mode in common SSL libraries such as Amazon's s2n, GnuTLS, mbed TLS, and wolfSSL.

OpenSSL supports TLS 1.3

The most popular OpenSSL library released version 1.1.1, the first version to support TLS 1.3.

Encrypted DNS

RFC 8484 ratifies the DNS-over-HTTPS (DoH) protocol. DNS over TLS (RFC 8310) is still in the draft proposal stage at the time of publication.

Distrusting Symantec

Major browsers, such as Chrome and Firefox, remove trust in the Symantec certificate authorities after discovering bad security practices in early 2017.

Encrypted SNI in Firefox

Mozilla announces they will support the ESNI draft protocol in the nightly builds of their Firefox web browser.

2018

Google Secures Email

Google is the first to enforce the MTA-STS policy, defined in RFC 8461, which secures email by validating mail server certificates and mitigates MITM attacks.

Kazakhstan Intercepts TLS

The nation of Kazakhstan briefly "tested" the interception of SSL/TLS traffic for a portion of its citizens after asking them to install a government issued root certificate.

Network Time Security

The new RFC for securing the open Network Time Protocol (NTP) inches closer to becoming final. The current draft uses TLS to authenticate and secure network time requests.

First Malware Spotted using DoH

Somewhat inevitably, security researchers discovered that some malware samples had begun using encrypted DNS-over-HTTPS to avoid security controls.

Firefox Enable DoH

Mozilla announces plans to gradually begin enabling the encrypted DNS service, DoH, by default for all of its users in the US.

Minerva Attack on ECDSA

Researcher discover side-channel vulnerabilities in implementations of ECDSA in programmable smart cards and cryptographic software libraries.

NIST Lightweight Crypto Draft

NIST publishes its first draft on the recommendations for use of lightweight cryptographic algorithms in low powered devices such as IoT.

Free Managed Certs for Azure

Microsoft begins offering organizations free certificates for custom domains when they use the Azure platform to manage the certificates.

DTLS 1.3 draft 34

The latest draft to the proposed standard will bring most of the same security guarantees to UDP that TCP already enjoys with TLS 1.3.

No More TLS 1.0, 1.1

In January 2020 Chrome intends to remove support for old TLS protocols and will only support 1.2 and 1.3.

2019 2020

Introduction

Welcome to the Summary of the 2019 F5 Labs TLS Telemetry Report. This year, we expanded the scope of our research to bring you deeper insights into how encryption on the web is constantly evolving. We look into which ciphers and SSL/TLS versions are being used to secure the Internet's top websites and, for the first time, examine the use of digital certificates on the web and look at supporting protocols (such as DNS) and application layer headers.

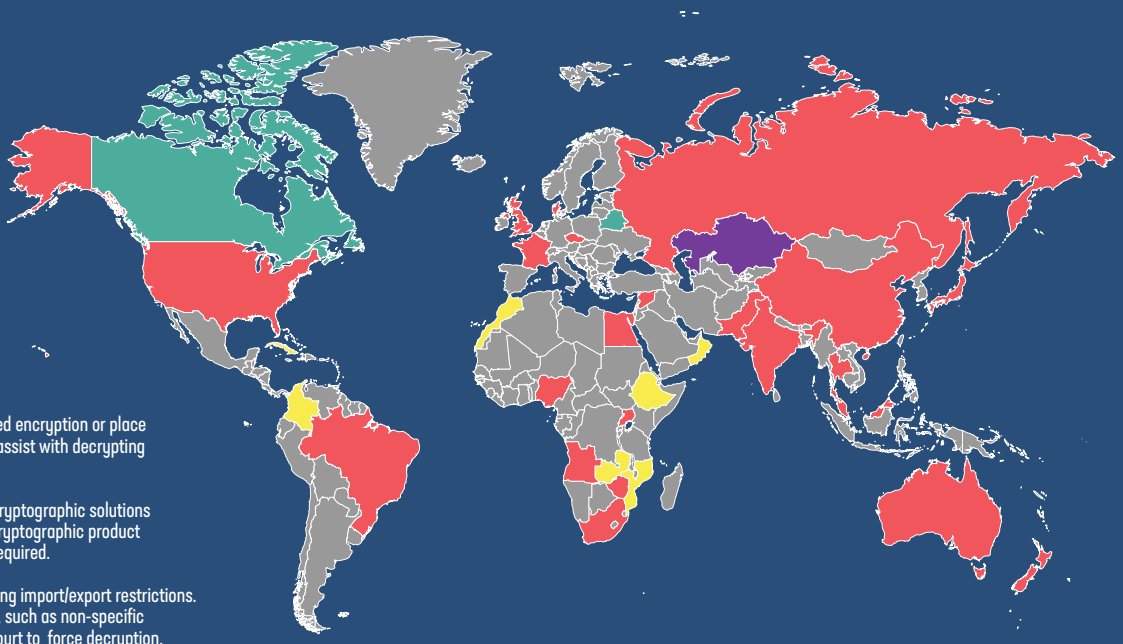
A lot has happened in the world of encryption since we published the 2017 TLS Telemetry Report.[i] Over the past two years, standards have been updated, browsers have evolved and a number of new protocols have been released that aim to secure all the remaining cleartext protocols still in wide use today. These new protocols don't come without their share of concern, however. In early 2019, security researchers found the first malware sample making use of the emerging Domain Name System (DNS) encryption protocol, DNS-over-HTTPS (DoH).[ii] Clearly, threat actors waste no time in using the latest encryption advances to their advantage.

MAJOR BROWSER VENDORS WILL BEGIN DROPPING SUPPORT FOR TLS 1.0 AND 1.1 IN EARLY 2020.

Meanwhile, the global debate between technology providers and governments (also known as Crypto Wars 2.0) continues to rumble on. Governments are increasingly trying to control how encryption is used, and we frequently see poorly written (or purposefully vague) legislation introduced. Many argue this is an attempt to either blatantly or surreptitiously introduce back doors into encryption. And the topic of conversation has shifted from capturing terrorists and cyber criminals to identifying and arresting those responsible for distributing child exploitation material.

FIGURE 1: GLOBAL MAP OF COUNTRIES WITH CONTROLS OVER THE USE OF ENCRYPTION

DATA SOURCE: HTTPS://WWW.GP-DIGITAL.ORG/WORLD-MAP-OF-ENCRYPTION/



- Countries which have outlawed encryption or place an obligation on providers to assist with decrypting communications.
- Only government controlled cryptographic solutions (e.g. VPN) is allowed, and/or cryptographic product licensing and registration is required.
- Cryptography is listed as having import/export restrictions. Other factors may be present, such as non-specific legalisation may be used in court to force decryption.
- Global standard deliberately weakened or subverted.

Countries such as the UK, Australia, and France have created new laws specifically designed to force providers to assist with data decryption. While many countries regulate the export of cryptographic products, China and Russia require government approved (licensed) use of encryption such as VPNs and, in the case of India, encryption is limited to a maximum key length of 40 bits without express prior permission.

IN JULY 2019, F5 LABS INVESTIGATED THE INTERCEPTION OF HTTPS TRAFFIC BY THE KAZAKHSTAN GOVERNMENT.[iii]

While governments around the globe ponder their position on the use of encryption, new protocols are rapidly being developed and adopted that improve our online security but also reduce visibility for those who believe they need it. *One thing is certain: the global debate over encryption is far from over.*

HTTPS Everywhere?

Chrome, the most widely used web browser, now fetches over 86% of web pages over secure HTTPS connections.[iv] That figure approaches 100% for Chrome OS-based devices when accessing Google properties like Gmail. For Firefox, HTTPS page loads are slightly lower but still at an impressive 80.5% average.

86% **ALMOST 86% OF ALL PAGE LOADS OVER THE WEB ARE NOW ENCRYPTED WITH HTTPS**

In our 2017 TLS Telemetry Report, we found that web servers preferred to use TLS version 1.2 around 62% of the time. In 2018, this figure was up to 89% but by the end of 2019, it had dropped significantly and was preferred by only 66% of web servers. The reason for this is entirely positive, however. Of the Alexa top 1 million sites, almost a third now accept TLS 1.3 connections (see Figure 3). This is an impressive proportion, considering the newest iteration of TLS is just over one year old. A likely reason for this relatively quick adoption is the speed with which the major browsers and content delivery networks (CDNs) have adopted it. That being said, cloud-native services in some leading cloud providers, including Amazon's Elastic Load Balancer (ELB), do not yet support TLS 1.3.

TLS 1.3 HAS SEEN RAPID ADOPTION AND IS NOW ACCEPTED BY 32% OF WEBSITES IN THE ALEXA TOP 1 MILLION.

FIGURE 2: AVERAGE (WEIGHTED) PERCENTAGE OF PAGE LOADS OVER HTTPS FOR CHROME AND FIREFOX WEB BROWSERS

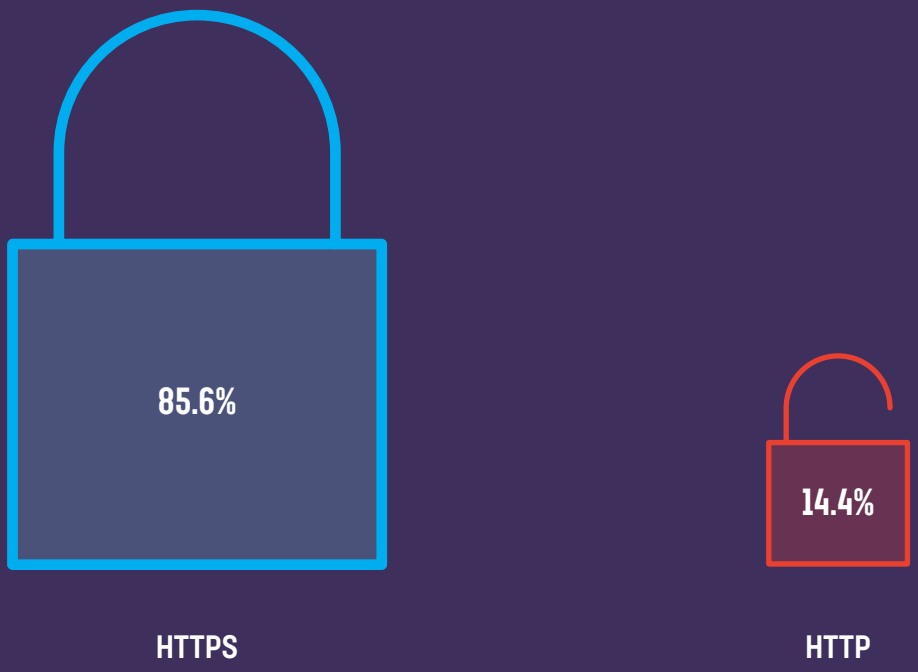
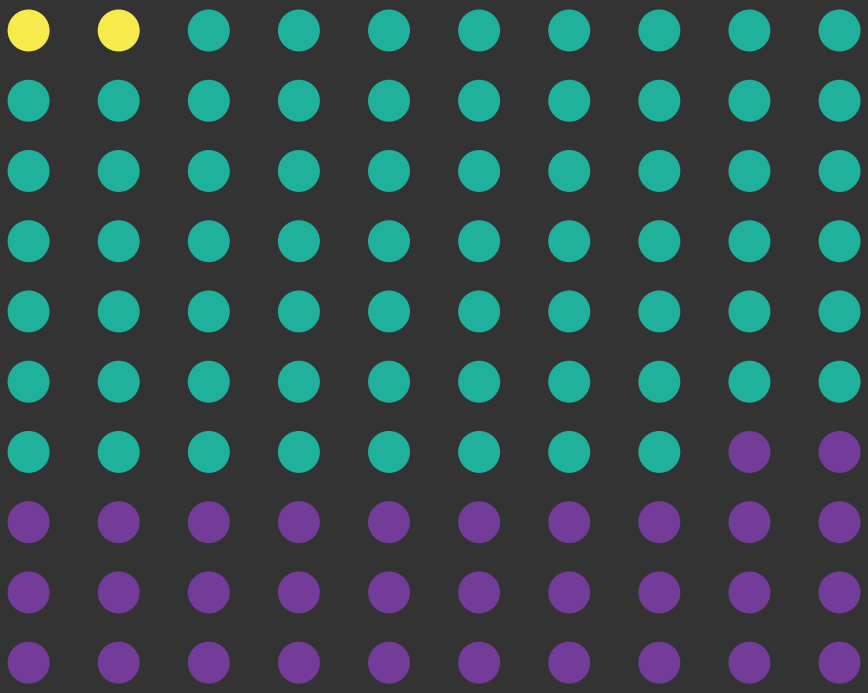
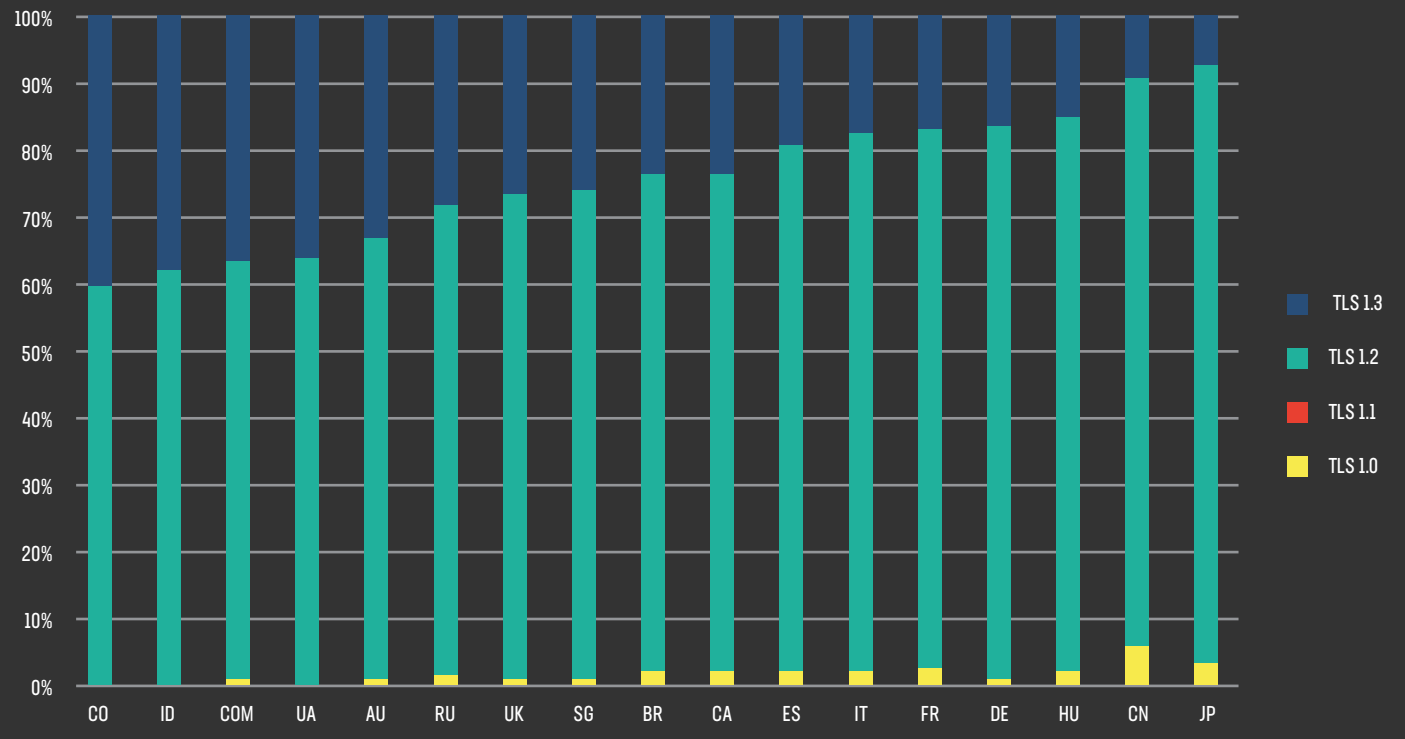


FIGURE 3: PREFERRED PROTOCOL VERSION SELECTED BY ALEXA TOP 1 MILLION SITES



TLS 1.3	32%
TLS 1.2	66%
TLS 1.1	0%
TLS 1.0	2%
SSL v3	0%

FIGURE 4: DISTRIBUTION OF TLS PROTOCOL VERSIONS ACROSS A SELECTION OF POPULAR TOP-LEVEL DOMAINS



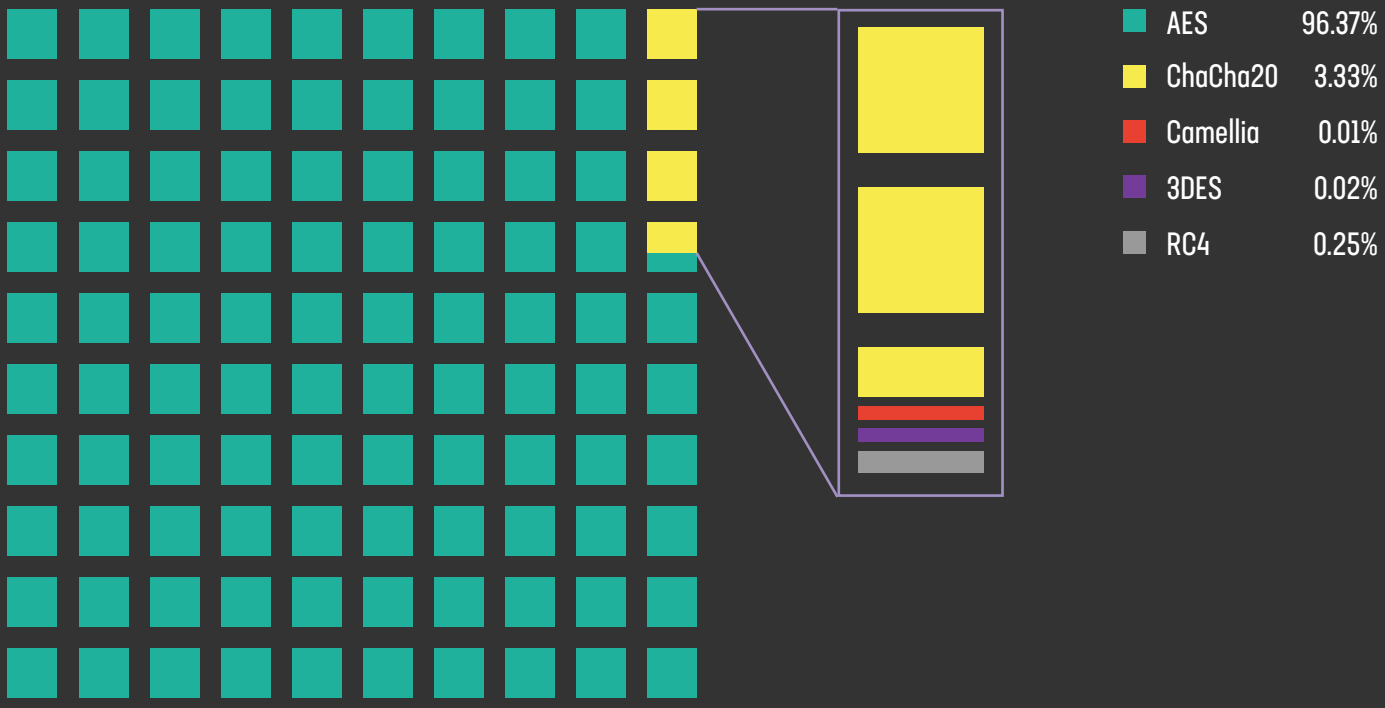
Protocols Across the World

Examining protocols by the top-level domain (TLD) of a website allows for a naïve comparison of how HTTPS is deployed across the globe. For example, the United Kingdom's TLD .uk has 72.6% of its sites offering TLS 1.2 as the most up to date version they support. Only 26.4% accept TLS 1.3.

AES Domination

Once the client and server have chosen the TLS version over which to communicate, they must then agree on which cipher suite to use. The one the server ultimately chooses may not necessarily be the most cryptographically secure option presented. Instead, the server decides which to use based on a combination of security, performance, and whether the workload can be offloaded to hardware.

FIGURE 5: DOMINANCE OF THE AES SYMMETRIC CIPHER

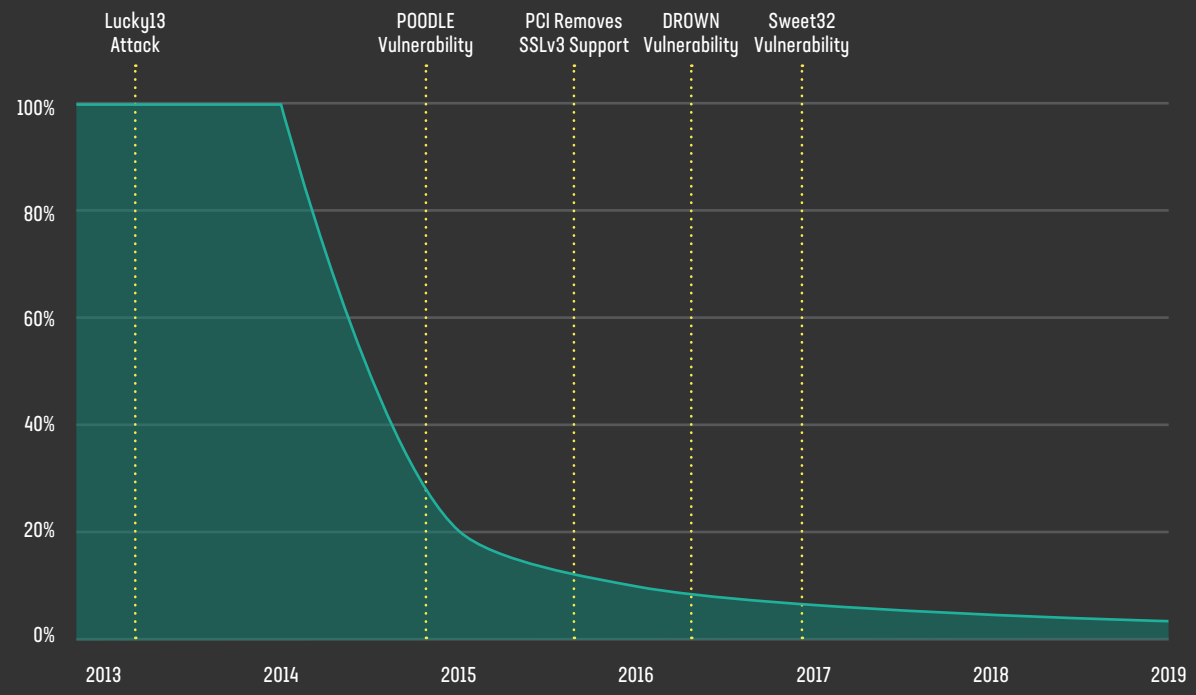


AES IS USED FOR OVER 96% OF TODAY'S ENCRYPTED HTTPS WEB TRAFFIC.

The Advanced Encryption Standard (AES) cipher is still the most widely chosen symmetric cipher across the web.

In fact, if we combine every possible cipher suite and ignore things like certificate type, key length, and hashing algorithms, AES accounts for over 96% of today's encrypted web traffic.

FIGURE 6: WEB SERVERS IN THE ALEXA TOP 1 MILLION ACCEPTING SSL V3 CONNECTIONS



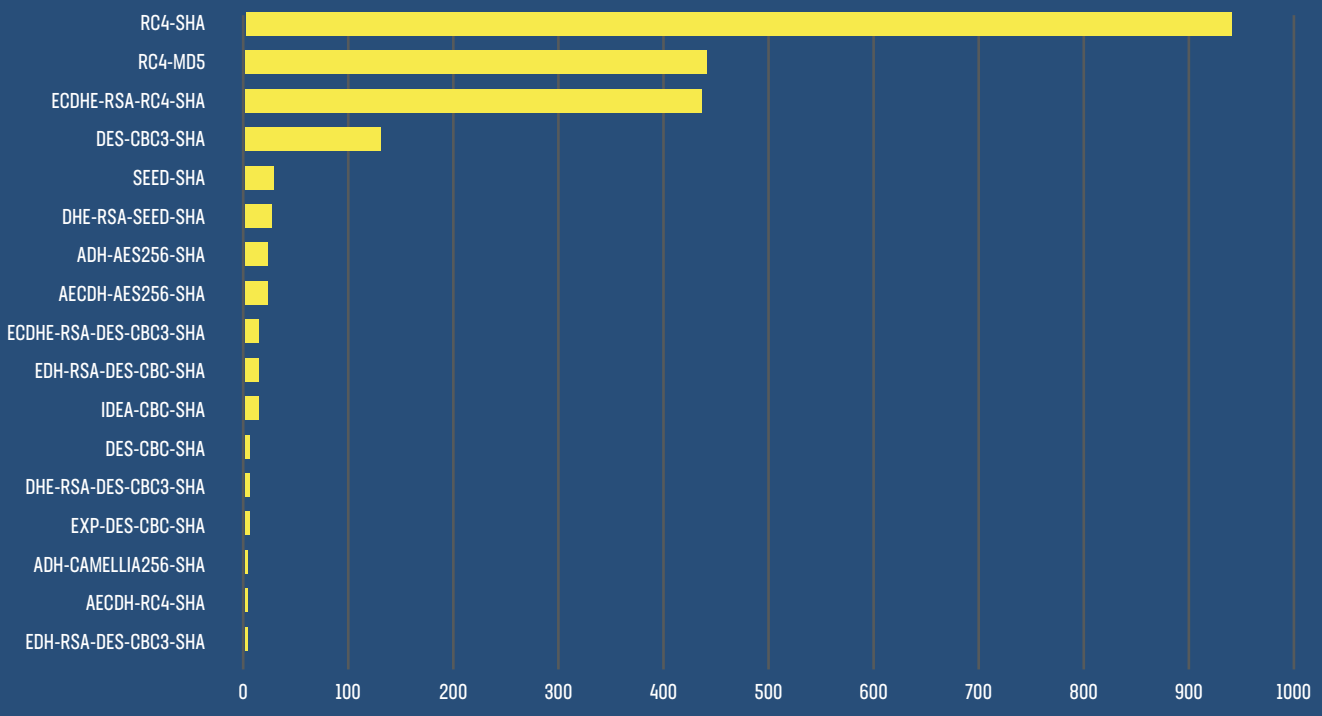
The Legacy of Legacy Protocols

Looking at a server's preferred protocol—typically, the highest SSL/TLS version supported by both the client and server—does not tell the whole story, however. Servers must often support legacy protocol versions lest they cut off access to users running older clients (for example, IE on Windows 7). This is why many web servers continue to accept connections on SSL v2 and SSL v3 despite also offering newer, more secure TLS versions.

IN 2014, 98% OF THE WEB SERVERS ACCEPTING HTTPS CONNECTIONS STILL ALLOWED THE USE OF SSL V3. THIS CHANGED RAPIDLY IN OCTOBER 2014 WHEN THE POODLE VULNERABILITY WAS ANNOUNCED.

In 2014, 98% of the web servers accepting HTTPS connections still allowed the use of SSL v3. This changed rapidly in October 2014 when the POODLE vulnerability was announced.[v] Since the

FIGURE 7: STRONGEST CIPHER SUITES AVAILABLE FROM SOME OF THE ALEXA TOP 1 MILLION SITES



handshake in a TLS connection is not encrypted, it is possible for an attacker to trick the server into thinking that the only protocol the client supports is SSL v3. Once the client and server finish their handshake using this legacy cipher, the attacker can perform padding oracle attacks against SSL v3 to recover the plaintext data.

Weak encryption algorithms and hashes can also be found on more than 2,000 web servers in the Alexa top 1 million sites. Since our scanner records the cipher suite that the servers ultimately chose to negotiate, the figures in Figure 7 represent the most secure option available for a particular website.

At the end of 2019 F5 Labs joined the GitHub Security Lab collation and as part of our new TLS Telemetry report.

The use of third party libraries is on the rise. Using them safely, however, requires that developers remain up to date with recommended best practices. As part of the **Security Lab** coalition, we asked **GitHub** to help us investigate the use of OpenSSL in open-source applications. They used their LGTM code analysis tool to examine the use of the world's most popular TLS library in 9,435 open source projects.

One of the most crucial parts of TLS is verification of the hostname. This has been under great scrutiny since incorrect implementations have been found in widely used software. This is, in part, due to older versions of OpenSSL having no built-in hostname verification. Modern versions of OpenSSL have corrected this and new functions are available specifically to validate hostnames. Unfortunately, adoption of these functions has been limited since they are available only in newer versions of OpenSSL which many developers will not proactively seek out to use.

Developers are frequently performing no hostname checks at all or are manually checking it in their code, against OpenSSL recommended practices. The recommended way to check the hostname inside a certificate is to use the `SSL_set1_host` or `SSL_add1_host` functions. We found that out of all the analysed projects only 6 used these functions. Alternatively, the `X509_check_host` function may be used but we found that only 32 projects were using this. This means that less than 1% of analysed projects were using OpenSSL recommended methods to validate hostnames.

Less than 1% of analysed projects are following OpenSSL recommendations for hostname validation

Developers must ensure that they fully understand the use of third-party libraries particularly when it is to perform critical security function such as authentication and validation.

These findings represent just a glimpse at the ongoing work between F5 Labs and GitHub researchers. For more details on the use of TLS in open source software, please see the full report.

A Matter of Trust

Arguably, the most important component of the TLS protocol is the use of digital certificates provided by the global public key infrastructure (PKI). They provide the most crucial of all security properties: trust. Each certificate contains information about how, when, and why the certificate owner should be trusted. This information is encoded and then cryptographically signed with the private key.

THE SHIFT TO ECDSA HAS BEEN CONSISTENT, WITH ALMOST 20% OF SITES NOW USING 256-BIT ELLIPTIC CURVE KEYS.

RSA has been the go-to signature algorithm for certificates for many years. The security of RSA derives directly from the length of the public/private key pairs. ECDSA elliptic curve-based certificates enjoy much smaller key sizes than RSA and offer equivalent security.

Sites that use RSA keys of less than 2048 bits pose a risk to users (6,300 sites we scanned used 1024-bits or less). Advancements in processing power and factoring algorithms allowed researchers in December 2019 to break 795 bit RSA key) using traditional (non-quantum) computing.[vi]

OVER 6,300 SITES IN THE ALEXA TOP 1 MILLION USE RSA CERTIFICATES WITH KEYS SIZES OF 1024-BITS OR LESS.

FIGURE 8: AVERAGE CERTIFICATE KEY LENGTHS USED AMONG OUR SCANS OF THE ALEXA TOP 1 MILLION SITES

KEY SIZE DISTRIBUTION		KEY TYPE
< 2048 bits	0.90%	RSA
2048 bits	73.57%	RSA
3072 bits	0.12%	RSA
4096 bits	6.91%	RSA
8192 bits	< 0.01%	RSA
256 bits	18.23%	ECC
384 bits	0.26%	ECC
521 bits	< 0.01%	ECC

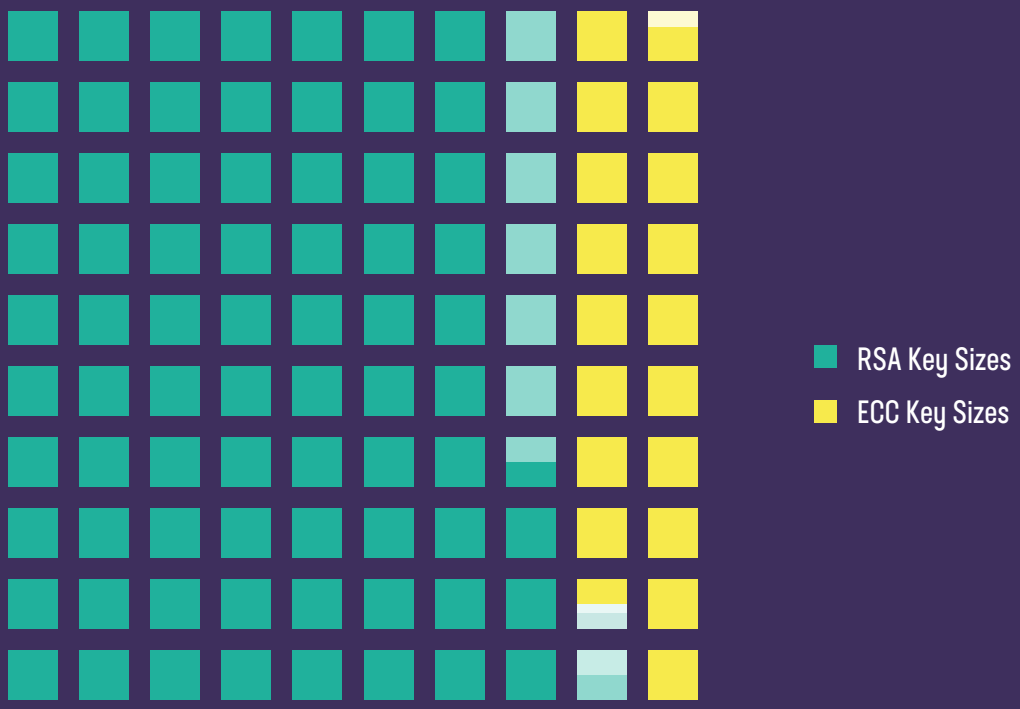
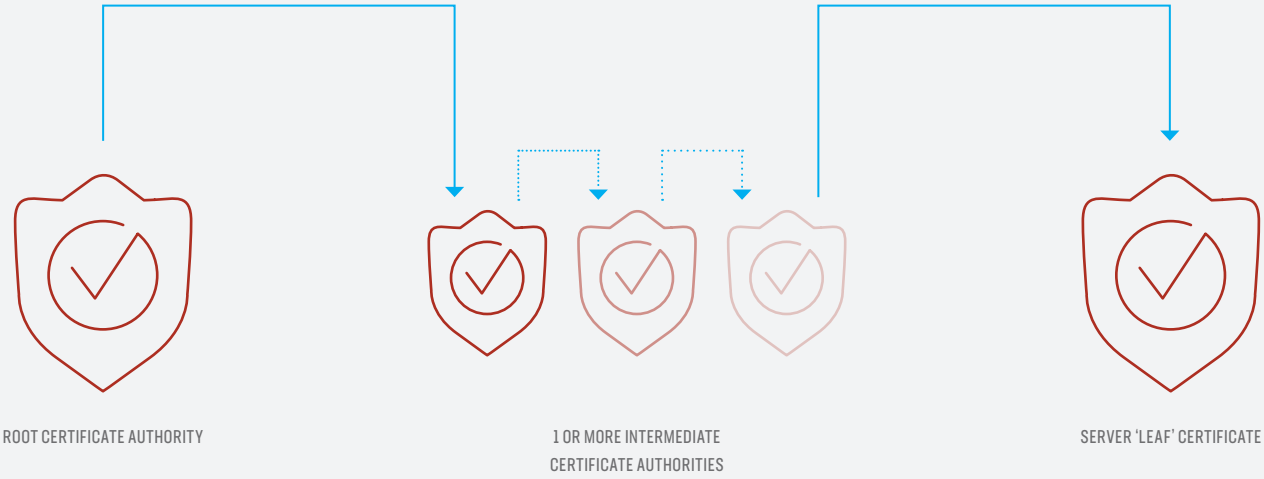


FIGURE 9: THE RELATIONSHIP BETWEEN ROOT AND INTERMEDIATE CERTIFICATE AUTHORITIES WITH SERVER CERTIFICATES

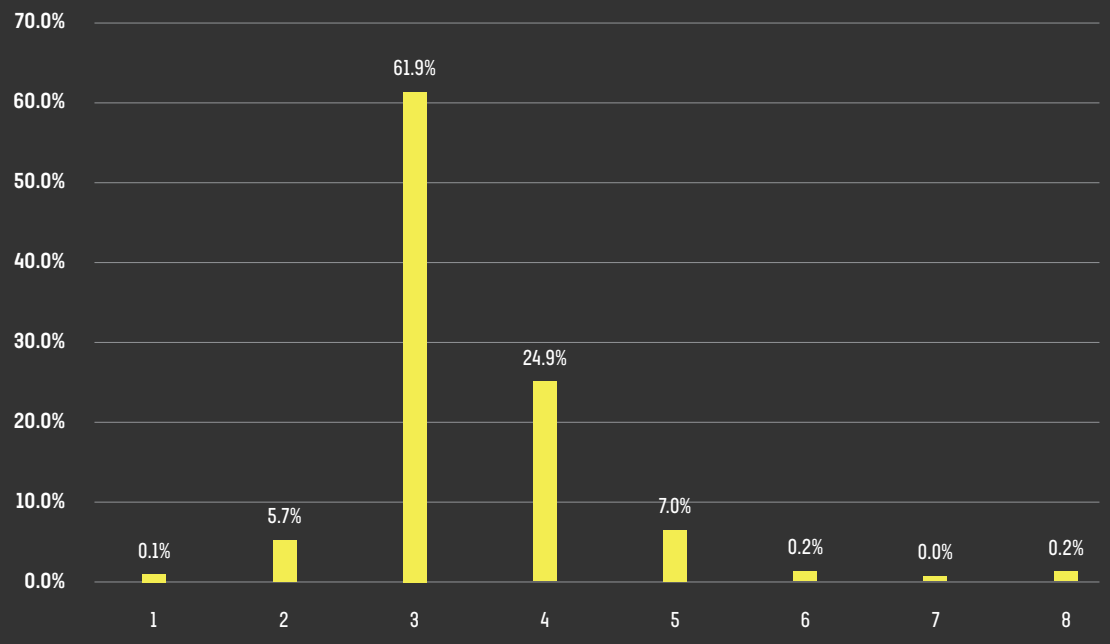


Certificate Authorities (CAs) verify the ownership of a domain and, in some cases, the organization itself before creating website certificates. Because the CA "root" certificate is embedded into our web browsers and operating systems, we implicitly trust any certificate that a CA digitally signs. Browser and operating system vendors must therefore ensure that only vetted certificate authorities are trusted in their products.

Let's Encrypt, the first free and fully automated CA on the web, was launched in late 2015 and has been a hit with web developers and operators. It now generates in excess of 1 million certificates per day and has become the number one certificate provider on the Internet.[vii]

For scalability and security reasons, root certificates are never used to sign web server certificates directly. Instead, the root CA signs the certificate of an intermediary CA who, in turn, signs the "leaf" certificate that is ultimately installed on to the web server.

FIGURE 10: AVERAGE CERTIFICATE-CHAIN LENGTH OFFERED BY SERVERS IN THE ALEXA TOP 1 MILLION SITES



When a web site sends its digital certificate to the client, it should also send all intermediate certificates that were responsible for signing it. This is referred to as the "certificate chain," and the number and order in which they're sent is important.

A certificate length of 1 means the web server is only sending back the leaf (server) certificate, which indicates either the certificate is self-signed or the server is misconfigured. A large number of certificates in a chain can cause performance issues since the client must verify each certificate. The largest number we observed in our scans was 34.

2.5% 2.5% OF THE ALEXA TOP 1 MILLION SITES SENT BACK AN INVALID ORDER FOR THEIR CERTIFICATE CHAIN.

Advanced TLS Security

Strong encryption is about far more than simply installing a certificate. Misconfigurations and legacy protocols can cause subtle problems that weaken the security of TLS. Increasingly, we see other protocols being used to provide a strong supporting foundation for TLS. Application layer security headers, such as HTTP Strict Transport Security (HSTS), ensure that web browsers only ever load a site securely. Its use continues to rise and appears to be doing so at an exponential rate, as shown in Figure 12. If the trend continues, we should expect all the Alexa top 1 million sites to use HSTS by mid-2021.

1.8% **ONLY 1.8% OF THE ALEXA TOP 1 MILLION SITES USE CAA RECORDS.**

To prevent arbitrary CAs from creating certificates for any domain they wish, website owners can configure Certification Authority Authorization (CAA) DNS records. When a CA receives a request for a new certificate, it must query DNS for CAA records. If CAA records exist for a domain, but the CA does not find itself listed within these records, then it must refuse to create the certificate.

The Alexa top 1 million sites revealed 225 different CAs defined in CAA records, but only 10, shown in Figure 12, accounted for over 95% of all results.

Many sites (67%) allow two or more CAs to create certificates on their behalf. The highest number we encountered was 15, attributed to a Brazilian government website which, ironically, doesn't even support HTTPS.

FIGURE 11: PREVALENCE OF HSTS HEADER USE ACROSS ALEXA TOP 1 MILLION SITES, 2014 – 2018

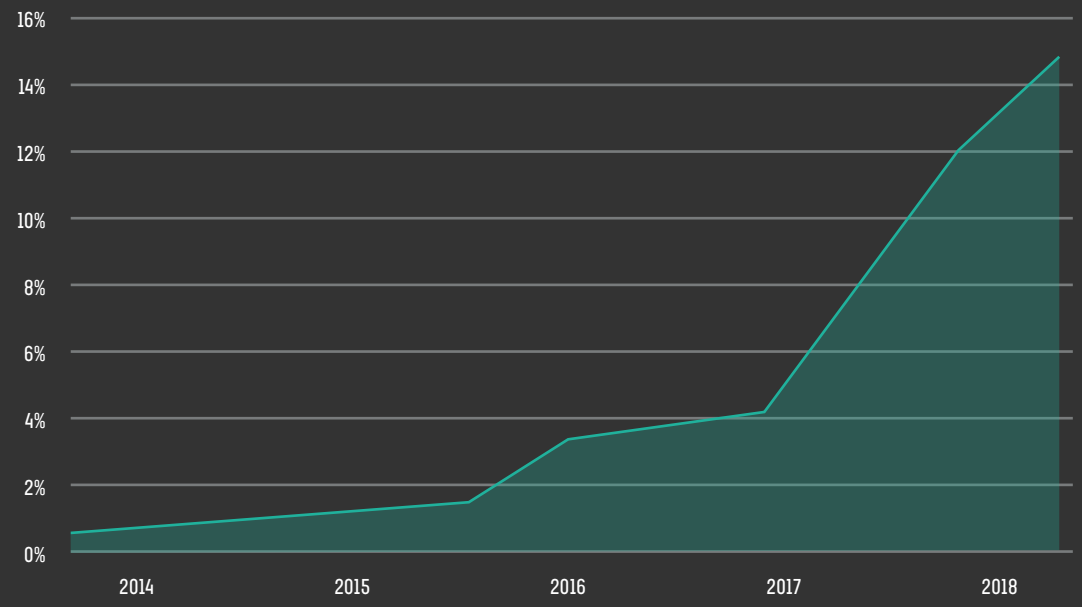
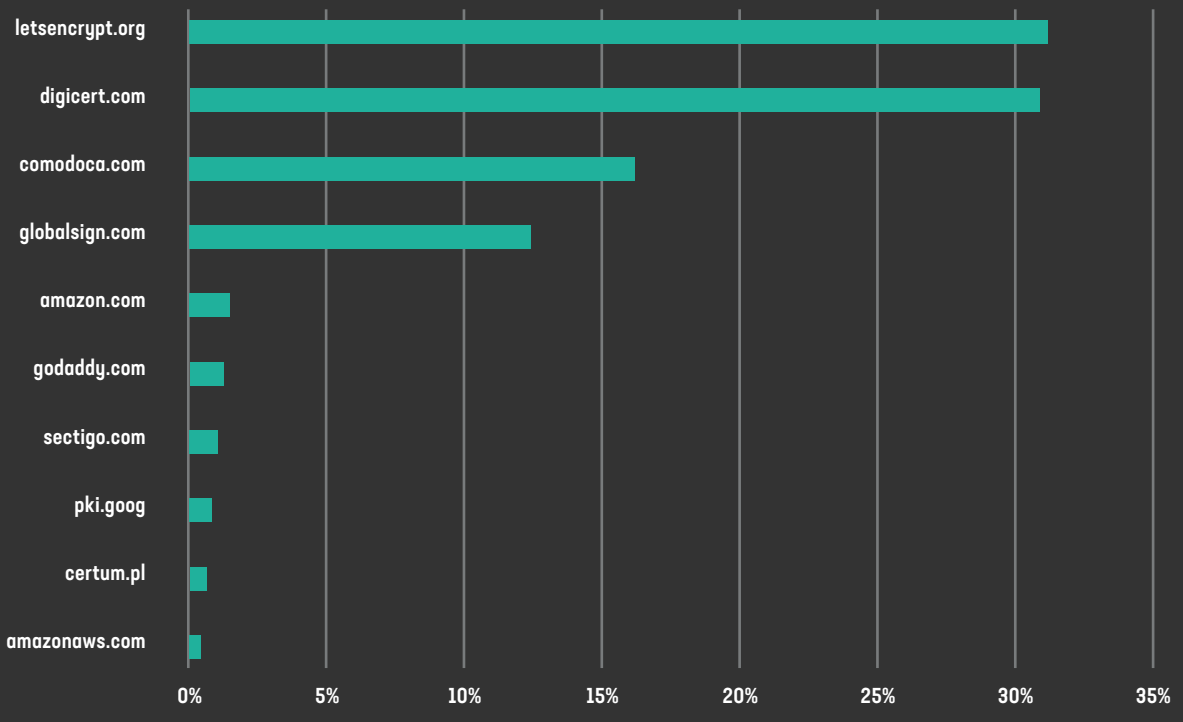


FIGURE 12: THE TOP CAs, ACCOUNTING FOR 95% OF ALL CAA RECORDS IN THE ALAXA TOP 1 MILLION SITES



Attackers Lurking in the Shadows

Encryption is an essential component of the web, but it comes at a cost. The same strong cryptography that affords us our privacy also makes it hard to identify and protect against malicious behaviour. From malware concealing traffic in encrypted DNS to abuse of certificates, it is critical to understand how threat actors are using encryption to their advantage.

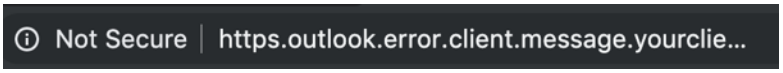
The world's most popular web browsers are helping improve the privacy and security of online users by marking unencrypted sites delivered over HTTP as "not secure." This is, however, only driving threat actors to use encryption and certificates in order to appear genuine and trustworthy.

We compared the malicious use of encryption to the wider web and found that domains that serve malware used a combination of legitimate public web services (such as blogging platforms and redirectors), valid certificates on malicious domains, and subtle tricks to conceal the true identity of the website. Phishing sites, used to lure victims into giving away their credentials, were even worse. The majority used HTTPS to hide traffic and appear genuine, and many sites attempted to imitate common financial institutions or ecommerce retailers.

IN JULY 2019, 57% OF MALWARE SITES AND 95% OF PHISHING SITES WERE ACCESSED JUST ONE TIME.

Of all the domains flagged as malware, 54% were served over HTTPS using valid certificates while 71% of phishing sites were provided over HTTPS. Threat actors frequently used domain-generating algorithms (DGAs) and popular sites to circumvent filters. In some cases, as shown in Figure 13, subdomains were used within the URL to imitate protocols and services. This trick was combined with very long addresses which had the effect of masking the real domain since it was lost beyond the end of the address bar. Although many users will spot the "Not Secure" indicator in Chrome, many peoople have simply been trained to look for HTTPS at the start of the address.

Figure 13
Very long website address as viewed in Chrome 70, Windows



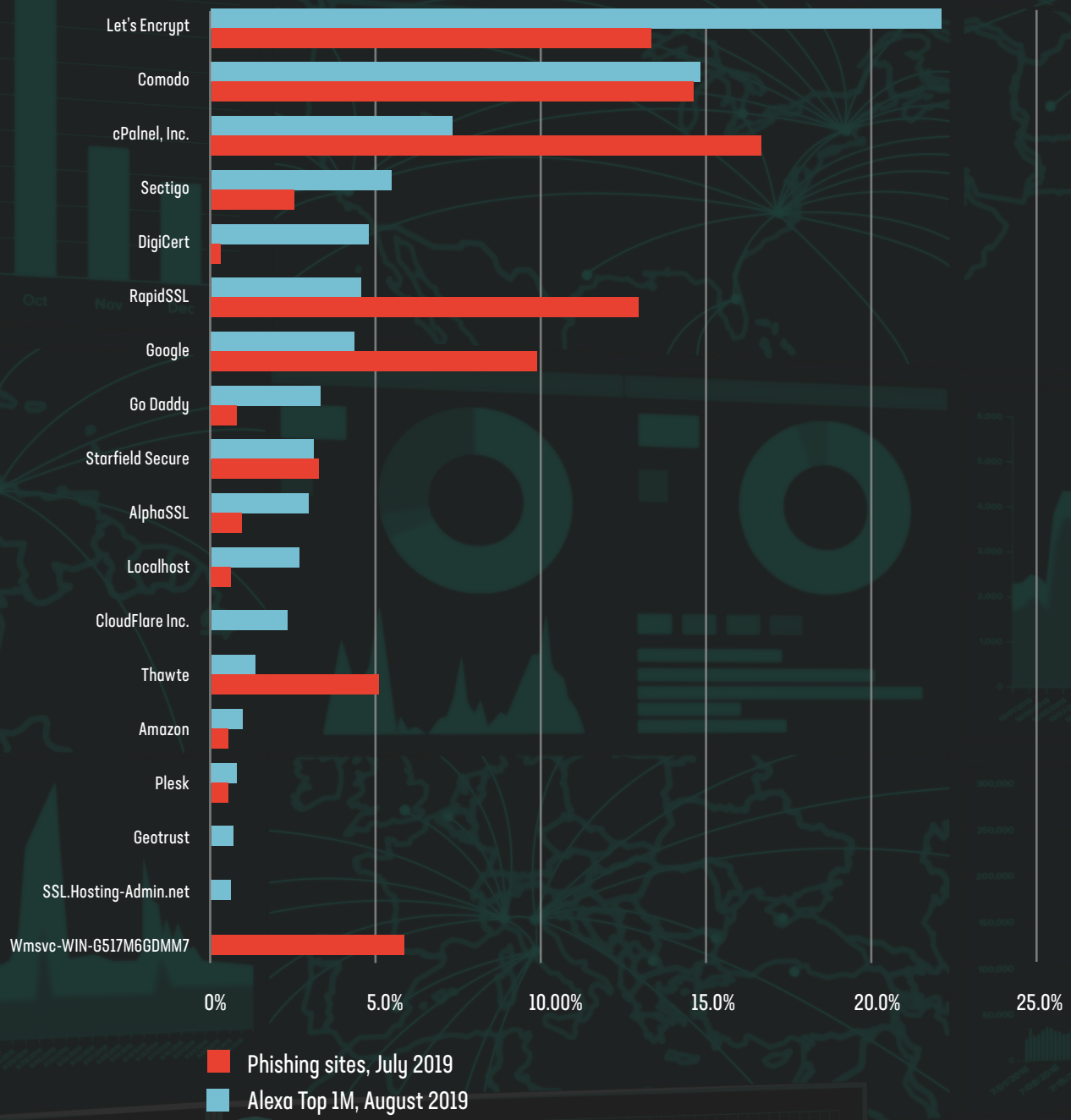
Attackers often host malware directly on a known service, such as Blogspot, or use URL shorteners such as duckdns.org. In 2008, Blogspot.com was cited as the number one host for malware online,[viii] and the same is still true today. We found that 43% of all requests to malware sites—by far the majority—were actually going to Blogspot. Pastebin.com, a legitimate service used to share code snippets, is similarly abused similarly. It is commonly used for hosting malicious files and is popular with all kinds of malicious actors (see our article on golang malware, which was hosted on Pastebin[ix]).

These sites use encryption and other security features to ensure their legitimate services are secure. But attackers can take advantage of the secure communication and user trust in these services in order to abuse them. The use of encryption and HTTPS here simply disguises the attackers' traffic as part of the legitimate service and makes it difficult to inspect the content.

An emerging tactic for malware authors is the use of other encrypted protocols. DNS-over-HTTPS (DoH) is a new protocol that tunnels DNS requests over the standard HTTPS port, 443. This allows attackers to blend in with legitimate network traffic. Despite the protocol still being in draft it has already been spotted in the wild in the Godlua and PsiXBot malware strains. We strongly expect this trend to rise.

36% **OVER 36% OF PHISHING WEBSITES USE CERTIFICATE AUTOMATION.**

FIGURE 13: THE MOST COMMON CERTIFICATE AUTHORITIES ISSUING DIGITAL CERTIFICATES FOR THE ALEXA TOP 1 MILLION SITES



The high churn rate of fraudulent sites being detected and removed from the Internet requires threat actors to automate their processes. We see evidence of this when we look at the most popular CAs used to create certificates for malicious sites.

While Let's Encrypt remains popular for both legitimate and malicious use, it is not the most common CA for use with fraudulent sites. Taking the number 1 spot for malicious usage is cPanel, a web server configuration and management tool that automates free TLS certificates in partnership with Comodo. RapidSSL and Google CAs also see high use likely due to the malicious adoption of services such Blogspot and Pastebin.

THE MOST POPULAR CA FOR THREAT ACTORS IS cPANEL, NOT LET'S ENCRYPT, AS MANY BELIEVE.

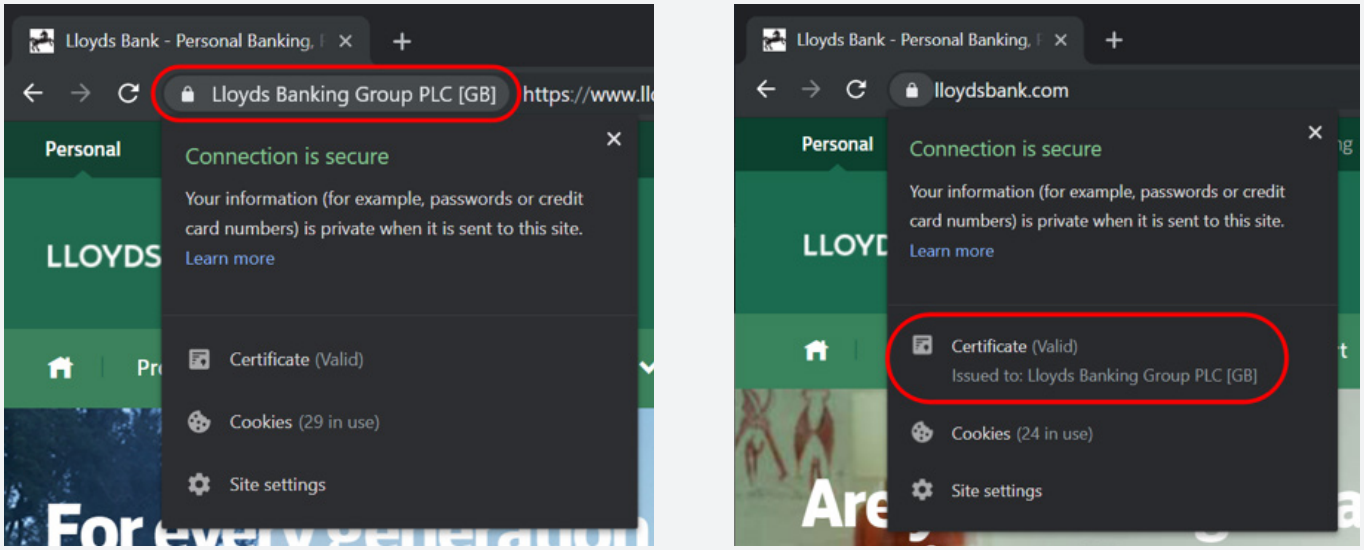
High trust "Extended Validation" (EV) certificates were supposed to help solve the phishing and fraud problem. The idea was that organizations could purchase a (rather expensive) EV certificate for their website after passing background checks. These certificates would then show the organization's name next to the standard padlock. Users would therefore, in theory, feel safe that they were dealing with a legitimate business.

But these high trust certificates have been frequently criticised for confusing users and doing nothing to prevent victims from visiting malicious sites.

21% OF PHISHING AND 89% OF MALWARE SITES USED HIGH-TRUST OV OR EV CERTIFICATES.

We found that 21% of phishing sites and 89% of malware sites used Organization Validation (OV) or EV certificates. While these numbers are almost entirely due to the use of legitimate services, it clearly illustrates one important point: if high trust certificates don't explicitly guarantee safety of a site, why use them?

FIGURE 14: AN EV CERTIFICATE AS SEEN IN FIREFOX 69 (LEFT) AND FIREFOX 70 (RIGHT)



Recommendations

Encryption standards are constantly evolving, so it's crucial to stay up to date with current best practices. Here are our recommendations to ensure that you are deploying secure web services as easily and securely as possible.

Keep TLS Current

TLS 1.3 is now more than a year old and over 80% of today's web browsers support it, according to caniuse.com.[x] The new protocol brings significant performance and security improvements, so you should be using it wherever possible.

Vulnerabilities can be discovered in cryptographic libraries, so ensure you are alerted when your web server, load balancer, or application delivery controller have updates to their TLS stacks. Have policies in place to allow you to patch rapidly.

Use Related Protocols to Bolster TLS

Use DNS CAA records to grant permission to only a few well-known CAs and monitor your DNS records regularly to ensure they have not been tampered with.

Using HSTS headers in your web app will prevent web pages from loading insecurely. Also, consider making use of HSTS "pre-load" whereby you instruct browser vendors to load your site over HTTPS without waiting to first see the HSTS header.

Monitor Certificate Transparency

DNS CAA records prevent mis-issuance of certificates for valid domains but fraudsters will often create certificates for a domain they own instead. Subdomains are then created which use a known brand or name. Monitoring Certificate Transparency (CT) logs is a useful way to be alerted to when your domain or brand is being impersonated by threat actors.[xi]

Automate and Orchestrate

HTTPS is now everywhere. This means more ciphers, keys, and certificates to manage and, with the increasing adoption of DevOps, the speed of change and deployment is constantly increasing. This means orchestration of digital certificates and creating internal policies that define the standards you must adhere to, such as minimum key length and cipher suites.

Mind the Gap

Many privacy and security gaps still exist, even when TLS is deployed correctly. Protocols, such as DNS-over-HTTPS (DoH), are emerging to help close these gaps and while they improve privacy for users of the web, they can also make it harder for enterprise security teams to identify and block malicious traffic.

Investigate how to disable DoH for enterprise networks or deploy your own internal DoH services for your users. These services will work with your web proxy and help filter out unwanted traffic.

The best TLS deployment in the world cannot prevent malicious code from being injected by client-side malware or compromise due to third-party scripts. Formjacking attacks can lead to devastating data breaches and the theft of personal and financial data. Novel methods are being developed to help combat this, including application-layer encryption and homomorphic encryption. We recommend understanding the limits of HTTPS and what gaps remain.

Conclusion

If there's one thing that can be said about encryption is that it's ever changing. Key lengths are increasing, certificates are becoming automated, governments are imposing restrictions, and new protocols are emerging. It is this constant change that poses a degree of risk to many organizations and their customers. It's unlikely that any new HTTPS websites are configured with deliberately weak cryptography. It is far more probable that once many web servers are configured, their TLS settings are never touched again, save for perhaps updating the certificate.

We have significantly expanded the scope of research with the hope that these findings can help inform decisions about how to safely deploy HTTPS web services. This summary only briefly looks at some of the key findings from our work. For a more detailed analysis and further advice on how to configure your TLS deployment securely see the full report on F5labs.com.

i https://www.f5.com/labs/articles/threat-intelligence/the-2017-tls-telemetry-report
ii https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/
iii https://www.f5.com/labs/articles/threat-intelligence/kazakhstan-attempts-to-mitm-itscitizens
iv https://transparencyreport.google.com/https/overview?hl=en
v https://www.us-cert.gov/ncas/alerts/TA14-290A
vi https://arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/
vii https://letsencrypt.org/stats/
viii https://www.cnet.com/news/blogspot-com-cited-as-the-no-1-host-for-malware/
ix https://www.f5.com/labs/articles/threat-intelligence/new-golang-malware-is-spreading-via-multiple-exploits-to-mine-mo
x https://caniuse.com/#search=tls%201.3
xi https://www.f5.com/labs/articles/threat-intelligence/fighting-back-against-phishing-and-fraud-part-2

We Want To Know What You Think

As security practitioners study how the Internet has evolved, the ways we manage new risks will mature. Attacks will also morph in turn, finding new ways to trouble us. In the meantime, we hope that the perspective and practices outlined in this report help you manage the latest incarnations of these older risks.

If you have feedback, data to share, requests for topics, or thoughts about our approach, please let us know. You can reach us on Twitter @f5labs, or email us at F5LabsTeam@f5.com.

APPLICATION THREAT INTELLIGENCE

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com